Pragmatic, Evidence-Based, HIT Security and Privacy Standards Will Drive Rapid Adoption and Provide the Most Effective Risk Reduction

Peter Tippett, MD, PhD,
Vice President of Technology & Innovation, and
Chief Medical Officer
Verizon

Testimony to The HIT Standards Committee, a Federal Advisory Committee to
Dr David Blumenthal, National Coordinator for Health IT
"Health IT Security Issues, Challenges, Threats, and Solutions"
November 19, 2009

Executive Summary

New standards are required to enhance security and privacy and to accelerate adoption of health IT. Current standards and methods are too complex, are based on dogma instead of science, are both ineffective and inefficient, and are too static. They are unable to evolve due to new stimuli or more simply put, "they can't learn from experience." The new standard should be risk-based and derived from real, actuarial evidence. It should be clear, concise, and mostly prescriptive, but it should also be general where hard evidence is lacking. Each of the elements and countermeasures of the proposed standard should be analyzed thoroughly for their independent countermeasure effectiveness, as well as for costs and likely infringement. Then the standard should be modified based on this risk analysis before it is first deployed. The standard must have an overriding "risk based exception" to allow for the large variance in threat, risk, exposure, business models, data models, and for inevitable change. Verizon and / or ICSA Labs have much experience designing and testing standards.

Reduce Cost, Improve Care

It is commonly accepted that the single most powerful intervention available to both reduce the crippling and increasing costs of healthcare and to improve quality is pervasive, practical and meaningful adoption of IT in healthcare. Scores of studies, erudite analytics and presidential addresses, among other efforts, have led to significant commitment by the US government to drive rapid and meaningful transformation of an industry that is a decade or more behind in the utilization of IT in managing the process of medicine.

Evidence-based Medicine

One of the mantras of the new revolution is "Evidence-based Medicine." We know that the broad application of the treatment and outcome evidence that is already understood and published could both save billions in healthcare costs AND improve quality. We also know that a treasure trove of new evidence is already collected, but not accessible enough to drive the analytics to yield still further improvements.

We postulate further that with better collection, standardization and sharing, we could build massively high–value data collections that could be expected to yield un-paralleled advances in both care effectiveness and efficiency. We can collectively taste the possibilities.

Challenges
Our two biggest challenges are:

1) Driving adoption of practical electronic records by the entire healthcare industry and

2) Effectively addressing both the perceived and real privacy and security problems.

In both cases we need to learn from the past while focusing on the pragmatic. Unfortunately, this isn't so easily accomplished when it comes to privacy and security. Please allow me to explain why.

Security & Privacy Getting Worse
Both the perception and the reality of digital security and privacy are worsening. Published information security and privacy failures are more and more common, impacting more and more citizens [1,2]. In the past several years, the majority of this malicious activity has been directed toward private information that can be monetized by the criminal, like credit card, SSN, and other personal identity information. The raw numbers of records at risk or records breached have grown every year during this decade. The 2009 Verizon Data Breach Investigations Report (DBIR)[3] reported the breach of some 285 Million individual records, representing only the investigations performed by Verizon, during 2008.

This increase has driven large, coordinated efforts by the Payment Card industry (PCI) to require that all players in the extended credit card ecosystem adhere to the PCI standard. The same DBIR [1] data shows that the PCI standard basically works. In the few cases where PCI seems to have failed, the "failures" can be classified mostly as: 1) no 3rd party was involved and the company misled itself into believing it met the standard to begin with, or 2) the standard was appropriately applied somewhere in the company, but the breach occurred somewhere else (a scope or discovery problem), or 3) something changed since the successful PCI evaluation that would have invalidated it and then the breach occurred.

PCI is Expensive and Costs are Increasing
The PCI standard is relatively prescriptive and straightforward, but with each passing year it gets increasingly expensive and disruptive. A 2008 Gartner survey [4] showed the average spending for level 1 merchants increased by nearly five-fold during the previous 18 months to an average of $2.7 Million. Ponemon [5] showed the 2008 costs at nearly $5 Million per large merchant.

This increase is mostly due to the increased requirements both in the standard, and in its interpretation (guidance). Requirements and guidance details are added, but components that do not reduce risk are not removed when they are found to be of little or no value. The standard does not include a cost–benefit or risk analysis of its elements and there is no feedback loop from field experience to remove ineffective, but expensive or infringing components. That is to say, there is no driver for both efficiency AND effectiveness. The updates that do occur are almost universally additive and are often increasingly difficult to deploy. This same model will inhibit, not enhance the speed of the required transformation to the digital healthcare ecosystem.

The Current State of IT Security Standards

Unfortunately, even with its inherent shortcomings, PCI is among our most modern and best security standards. Most others are worse in many respects. In order to achieve both excellent protections for our citizens, and rapid adoption of the digitized medical record healthcare, the upcoming security and privacy standard for Health IT needs to be even better than PCI.

Our IT security and privacy-related activities tend to be based primarily on gut feeling, dogma and logic pitfalls that too often lead to bad decisions, bad standards and wasted time and resources. Some of the pitfalls that have driven our dogmatic thinking include: the perfection problem, the focus on vulnerability, the dependence on binary computer engineering logic instead of community and population disciplines, conflation of problems and countermeasures, and driving decisions and standards by a WIBeHI ("Wouldn't It Be Horrible If") reasoning model. Most standards (and security practices in general) can be characterized as being derived from a "Dogma-Driven Approach".

The Dogma-Driven Approach really has two significant drawbacks:

1) A Dogma-Driven Approach creates inefficiency. While we might be willing to suffer some inefficiency in order to reduce risk and increase the probability of maintaining privacy, in a complex system (like a health information network), inefficiency has an adverse effect beyond wastefulness – inefficiency actually increases the frequency of failure [6]. Complexity also increases the probability of failure. Therefore poorly written or enabled standards are doubly counterproductive; they distract us from our charter to reduce risk and inhibit rapid transformation.

2) Dogma-Driven Approaches are sometimes just plain wrong. For example, the best risk models and scientific evidence suggest that we are as wrong about many of our most firmly held security and privacy beliefs as we were about the value of leaches in curing tuberculosis and broken bones. Data and risk models [1,2,3,6,7,8,9,14] are now beginning to show us that:

1) Passwords longer than about 5 characters do not reduce risk in any meaningful way among communities of users.
2) Encryption of data at rest in databases and other large systems, typically provide no value versus the large majority of hacking and malicious code threat scenarios.
3) The incremental benefit of applying security "patches" more rapidly is dramatically overstated.

4) End user devices like PCs, laptops, PDAs, and so on are orders of magnitude less important targets in the real world than is commonly perceived (and databases are several orders of magnitude more important than end user devices).
5) The protection of assets thought to be "non critical" is orders of magnitude more important than commonly believed.
6) The application of the basics, pervasively across enterprises with tools, techniques and processes that are already understood, reduces risk far more than expensive product or technology-driven efforts focused on the most critical parts of the system.
7) Intrusion detection systems are far less effective when deployed than expected, while log analysis has the potential to be far more effective than is commonly believed.
8) 90% of large event losses involve failures of discovery (an organization knowing its architecture, major data flows, major connectivity, location of sensitive data on servers).

And the list goes on.

Proposed Solution

Risk-Based Standard with Feedback Loop

What we need is an alternative. We need an alternative that focuses on the evidence where available, and which utilizes sound risk models where the data is sparse. We need to follow the most fundamental rule in medicine: "First, Do No Harm." We need to learn from the experiences of the other industries, leverage their successes and avoid their failures. We need to be prescriptive where the risks are real and the countermeasure evidence is strong and, at the same time, provide broad goals and allow for latitude where the science is sparse or the evidence is weak. We need this risk-based standard to proactively evolve based on feedback of successes and failures in the community. The feedback loop needs to be able to both add new requirements and remove them. It needs to be able to provide interpretation of standards that lead both to more complex solutions, and to simpler ones. In essence, it simply must be an organic, living, breathing system, which responds to stimuli and situations, rather than the rigid and unyielding list of checkboxes we have tried in the past.

Above all, the new standard must have a "risk basis" like HIPAA which means (among other things) that a risk analysis must be part of the requirements of the standard. It also means that the fundamental requirement of the standard must be to reduce risk, not to explicitly meet every line of the standard nor its guidance. Furthermore, it must be possible for the target organization to show that any particular requirement of the standard either does not apply to it, or that the threat or risk is not relevant to its situation, or that the organization is reducing the particular risk by alternate means. In any of these cases, the organization should be able to "pass" the standard the same as if it met all of the explicit requirements of the standard and / or its guidance.

We need to realize that standards created for military and secret agency risk during a cold-war era are mostly unrelated to privacy, and are often ineffective and counterproductive in the massively interdependent computing ecosystem that defines networked and mobile IT of today and tomorrow.

In short, we need to apply the same evidenced-based approach to reducing risk in IT Security as we believe is best in the new move to evidence-based healthcare.

Evidence-based Security and Privacy Standard
An Evidence-based Security Standard requires three elements:

1.) A simple, risk-based framework of security and privacy controls.
2.) A means (technology and process) to share incident and failure information,
3.) A process for updating and evolving the framework of controls and the interpretation and application of the framework (guidance) based on incident and failure information.

When you look at these three elements, what we're really describing is the implementation of scientific method. In IT, as in healthcare, the natural sciences, and every other endeavor for knowledge mankind has embarked upon - without a systematic and scientific approach, we are left only with dogma and the increased probability of failure.

How Can We Create Evidence-based, HIT Security and Privacy standards?
We need to crawl before we can walk, before we run. We need to focus on the pragmatic, by creating a body of oversight that will be the custodians of this evidenced-based standards process.

Our recommendation is to create a standard that utilizes the efficiency of evidence-based security. This would involve the three simple concepts that work together to provide a feedback loop that evolves and improves security and privacy rapidly at first, and then adjusts and improves continuously over time:

1.) Make a simple framework for security controls that is mostly prescriptive, but is also very flexible.
Use PCI as a model. Do not use current government or military standards as the framework or for parts of the framework. Make sure the framework is prescriptive and explicit where issues are well understood and evidence-based data exists, and is general where organizations implementations vary, or where the countermeasure effectiveness data are lacking. Make sure that an overriding risk standard is included that runs according to the following lines: The organization shall perform a risk analysis and shall take appropriate action to effectively address the identified risk. And, "Every part of this standard may be considered to be satisfied if a risk analysis shows that the threat does not apply, that the risk is not significant or applicable to the particular situation, or that one or more alternate means of adequately mitigating the risk are in place".

The standard needs to accept and encourage the use of current technologies, countermeasures, protocols and methodologies. For example SSL, SSH, PKI, SMTP, and dozens of other common and well understood technologies should be acceptable and encouraged with the right mixture of controls.

Like PCI, enable the industry to provide assessments and compliance evaluations (with penalties for non-compliance) to that control framework. However, unlike PCI, require or provide these assessors with training in risk basics, as well as in risk-based decision making.

After the initial framework for the standard is developed, commission one or more risk analytic evaluation of it. The analysis should assess each proposed security and privacy control versus 3-5 common use cases (For instance, HIE, Hospital EMR, Small Practice EMR). These evaluations should specifically look for gaps AND should look for areas of too much depth. In addition this analysis should also seek less expensive, more rapid or less infringing means of addressing the same risks with different combinations of controls. The standard should encourage use of these simpler control packages.

The evaluation should examine each component of the standard according to its countermeasure effectiveness versus known top 10 threat scenarios, and then perform an economic analysis according to the likely cost of implementation and maintenance of the control. Optimize the standard for rapid, easy implementation and holistic, balanced risk coverage. The baseline standard should drive efficiency by requiring what is essential, not what is best.

Deploy the standard as a series of progressive standards. Start with the mix of countermeasures that provides the most rapid risk reduction for the citizens with the least cost, infringement and time to deploy for the target organizations.

2. Design Recurrent Data Collection and Feedback into Standard

As part of the evidence-based security standard, provide the people, process, and technology for the semi-anonymous collection of incident and control failure information. Use the incident and failure information as the basis for risk analysis and data that drives feedback for the evolution of the control framework.

This analysis should include all of the reported incidents annually. Publish the data including analytics of root cause, simplest avoidance controls, trends, etc. Use feedback on the published report, the actual loss experience, information from the audit and compliance process, and a reiteration of the framework development process in step one above to drive new guidance and versions of the standard. Make sure that the new guidance as well as any changes to the standard improve the deployed countermeasures, both by providing more countermeasures where appropriate, more explicit guidance or more rigorous interpretation AND by reducing complexity, rigor, and prescribed countermeasures where the data does not support continued use.

3. Update the audit and compliance process to reflect the new evolution of the standard.

Roll out the standard as crawl (v1.0), walk (v2.0), run (v3.0). Instead of defining v2.0 or 3.0 now, wait and evaluate the crawl requirements, implementation issues, feedback, costs, effectiveness, work-around, compensating controls, risk analyses and other data provided by users, assessors, and others. Then fine-tune everything for the 2.0 release. V1.0 should provide the most risk reduction with the least effort, cost and infringement. V2 and v3 should derive their new controls from actual data from the community gained by the incident and control-failure analysis and collection described above.

Two Case Histories: ICSA and Cybertrust Certifications

Both the Cybertrust division of Verizon and ICSA Labs have developed and deployed similar risk-based standards, assessment frameworks and certifications with feedback loops and a dynamic methodology whose new criteria are based on formal metrics and feedback.

ICSA Labs focuses on security and privacy standards, as well as the testing and certification of technology products with network connections. ICSA Labs (formerly NCSA) has created and managed over a dozen different certification and testing programs over the past 20 years. ICSA has tested and certified the security and privacy of products from more than 400 companies since 1989. A study of the performance metrics of a range of these certifications and labs testing results was recently published [10]. The data show that even simple, version 1.0 style testing can reduce risk dramatically while allowing a target community to accelerate its growth.

ICSA Labs intends to provide similar services surrounding the meaningful use criteria, interoperability, security and privacy criteria for Health Information Systems, including HIE, EMR, EHR and related IT products used for Health Care in the United States as required by the 2009 American Reinvestment and Recovery Act.

Verizon (under the TruSecure and Cybertrust brands) has provided a continuous, dynamic certification program which has included over 1,000 enterprises, with over 120 in the healthcare, since 1993. Three different studies have been performed comparing companies which were certified under these programs, companies that were engaged in the programs, but not yet certified, and several thousand "control" companies that were unrelated to the Cybertrust Risk Management or Cybertrust Security Management Progams. All three studies measured the relative risk reduction of certified companies versus the other two groups. All three studies showed very large reductions of risk (typically 40-fold reduction (over 97% reduction) of risk between certified enterprises and those in the control group for risks related to malicious code, viruses, and hacking.

ICSA Labs, the Medical Transcription Industry Association (MTIA) and Verizon, along with numerous Medical Transcription Service Organizations (MTSOs), recently formed the Medical Transcription Service Consortium [11] to design and provide a secure,

private exchange of transcribed medical records between providers, and from providers to the rest of the digitally-enabled medical ecosystem. The exchange will be deployed relatively rapidly using the principles described above with security and privacy driven both through design and by certification of the appropriate providers as described above. The security and privacy standards for this system and its member/providers will meet or exceed the new HIT security requirements when they are final. But the infrastructure and its providers will get more rapidly to market by exceeding current standards and by following a risk-based, dynamic approach with the most important risks addressed first. By 2010, this consortium expects to be moving as many as hundreds of millions of the most important of all medical records – the summaries, analysis, thoughts, and plans provided by the physicians themselves through their dictated notes.

Conclusion

We need to rigorously test every assumption that drives every element of every standard to discern which are driven by dogma and which by data. We need to focus on the goal of reducing risk -- which means we need to avoid false logic based on vulnerabilities or threats or consequences in isolation of the other. We need to understand the logic pitfalls that lead to bad decisions, bad standards and wasted time and resources, and which distract us from our charter to reduce risk and drive rapid transformation. And given the current economic crisis, we cannot afford to rely on anything other than that which will produce results -- evidence-based security.

By creating a risk-based standard, and providing for both designed-in feedback loops and an evidence-based, dynamic and continuous update cycle for both the standard and its implementation, and by providing for an emergency alert, "rulemaking," and testing processes – the worry of trying to "get it perfect" before deployment will be lessened. The security and privacy standard will be simpler to understand, train, deploy, and test against. Adoption and actual risk reduction in the community will be improved. Costs and infringement will be minimized. All of these things will streamline and accelerate the adoption of health IT -- which is the overarching goal.

REFERENCES:

1 DBIR 2008
http://www.verizonbusiness.com/resources/security/databreachreport.pdf
2 DBIR 2008 Supplement
http://www.verizonbusiness.com/resources/whitepapers/wp_supplemental-report-specifics-for-the-financial-services-food-beverage-retail-and-tech-services-industries_en_xg.pdf
3 DBIR 2009 –
http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf
4 PCI Compliance Remains Challenging and Expensive (2008)
Avivah Litan, Gartner Research
http://www.gartner.com/DisplayDocument?ref=g_search&id=672214
5 Ponemon 2009 PCI DSS Compliance Survey (2009)
Ponemon Institute, LLC
https://www.imperva.com/ld/ponemon.asp
6 How Complex Systems Fail (2000)
Richard I. Cook, MD
University of Chicago Cognitive technologies Laboratory
http://www.ctlab.org/documents/How Complex Systems Fail.pdf
7 Stronger Passwords Aren't
http://journals2.iranscience.net:800/infosecuritymag.techtarget.com/infosecuritymag.techtarget.com/2002/ciso/ciso-strongerpasswords08.shtml
8 Sweat the Easy Stuff
http://journals2.iranscience.net:800/infosecuritymag.techtarget.com/infosecuritymag.techtarget.com/2002/ciso/ciso-sweateasystuff08.shtml
9 Defense in Dept
http://journals2.iranscience.net:800/infosecuritymag.techtarget.com/infosecuritymag.techtarget.com/2002/feb/columns_executive.shtml
10 ICSA Study Published Nov 16,
http://www.icsalabs.com/sites/default/files/WP14117.20Yrs-ICSA%20Labs.pdf
11 MTSO Press release
http://newscenter.verizon.com/press-releases/verizon/2009/icsa-labs-and-medical.html
14 Calculating Risk
http://journals2.iranscience.net:800/infosecuritymag.techtarget.com/infosecuritymag.techtarget.com/2002/ciso/ciso-calculatingrisk08.shtml

Peter Tippett
Vice President of Technology and Innovation
Verizon Business

Peter Tippett is vice president of Technology and Innovation for Verizon Business and is the chief scientist of the security product testing and certification organization, ICSA Labs. An information security pioneer, Tippett has led the computer security industry for more than 20 years, initially as a vendor of security products, and over the past 16 years, as a key strategist. He is widely credited with creating the first commercial anti-virus product that later became Norton AntiVirus. Tippett is best known for his creation of enterprise risk metrics, and large risk intelligence and compliance management programs for enterprises.

Tippett served on the President's Information Technology Advisory Committee (PITAC) to guide U.S. efforts in healthcare IT, information security and computational sciences research. InfoWorld recognized Tippett as one of the 25 most influential chief technology officers for 2002. He has also won the Ernst & Young Entrepreneur of the Year award. Tippett has written many articles and papers on IT and information security and was the founding executive publisher of *Information Security Magazine.*

Tippett took up his current role following the 2007 acquisition of security specialist Cybertrust by Verizon Business. At Cybertrust, Tippett was the chief technical officer and was instrumental in developing the Cybertrust Security Management Program, which has served over 1,000 organizations for 12 years. He was also chairman of MD-IT, an intelligent transcription company.

Before Cybertrust, Tippett was the chief executive officer of the NCSA, then ICSA Labs, and was chairman of TruSecure, the largest private US security services company. In the early 1990s he directed the Enterprise and Security products group at Symantec. In addition to start-up and CEO positions, Tippett has led large software development, product management, production labs, technology research, and intelligence teams in his business career.

Early in his IT career, when he was founder and CEO of software company Certus International, Tippett pioneered and commercialized a string of now-common technologies, including what is now called the "rescue disk," code signing (hashing for execution control), trusted file execution, anomaly detection, and aspects of mail merge and the "un-do" command. He also created and sold the first cyber insurance to enterprises. Before the first PC was marketed, during the early 1980s, Tippett ran one of the largest open source (shareware) bulletin boards.

Tippett has a bachelor's degree in biology from Kalamazoo College, and holds a doctor of medicine degree and a doctor of philosophy degree in biochemistry from Case Western Reserve University. He has worked as an emergency room doctor and as a helicopter emergency physician in both Ohio and California. He still carries a current California physician and surgeon license. Tippett also worked as a lab technician for Nobel Laureates Robert Bruce Merrifield (who won the prize for chemistry in 1984) and Stanford Moore (chemistry, 1972) at Rockefeller University. He began his career as a commercial pilot and flight instructor and worked as a radio engineer at a US Top-40 radio station during college.

January 2009